Chapter 16
Configure Discard Interfaces

On the router, you can configure one physical discard interface, dsc. The discard interface allows you to identify the ingress point of a denial of service (DoS) attack. When your network is under attack, the target host IP address is identified, and the local policy forwards attacking packets to the discard interface. When traffic is routed out of the discard interface, the traffic is silently discarded.

You can configure the inet or inet6 family protocol on the discard interface, which allows you to apply an output filter to the interface. If you apply an output filter to the interface, the action specified by the filter is executed before the traffic is discarded.

To configure a discard interface, include the following statements at the [edit interfaces] hierarchy level:

```
[edit interfaces]
dsc {
    unit 0 {
        family (inet | inet6) {
            filter {
                output filter-name;
            }
            address address {
                destination address;
            }
        }
    }
}
```

Keep the following guidelines in mind when configuring the discard interface:

Only the logical interface unit 0 is supported.

The filter and address statements are optional.

Although you can configure an input filter and a filter group, these configuration statements have no effect because traffic is not transmitted from the discard interface.

The show interface command is not relevant for the discard interface.

Once you configure this interface, you must then configure a local policy to forward attacking traffic to the discard interface. For a complete discussion about using the discard interface to protect your network against DoS attacks, see the *JUNOS Internet Software Configuration Guide: Policy Framework*.

JUNOS 5.6 Internet Software Configuration Guide: Interfaces and Class of Service